【論文】

顔認証技術の社会化に伴う社会科学文脈における課題の考察
――表情認識AI「エモスタ」の発生プロセスと実践を題材として――

高　柳　寛　樹

はじめに

1995 年のインターネット爆発（高柳，2010）以降、情報テクノロジーの急激なスピードでの発展が続いている。これに伴い、1995 年以降に生まれた世代をデジタルネイティブ（高橋，本田，寺島，2008）（高柳，2017）として、それまでの世代とを分けて情報行動を考えることで整理する動きも多くなってきた。つまり、生まれながらにしてインターネットがあった世代とそうでない世代の違いである。ところで、なぜインターネットがそんなに大きなインパクトになったのかを論ずる必要もある。しかしこれには多くの先行研究があるため、ここでは紙幅を割かないが、筆者は一貫して、この 20 数年間において「オープンソースの精神」がもとになった「中間層」によるテクノロジーの主体的開発が行われてきたからであるという立場を貫いている（高柳，2010）（水越，2002）（古瀬，広瀬，1996）。つまり、それまで資本や権力によって独占されたきたテクノロジーがインターネットを通して「オープンソースの精神」とともに大衆化したために、誰でもが、極端には一人の個人でも、大資本や権力に勝るとも劣らない情報テクノロジーに纏わる開発を進めることができたのである。つまり、1995 年前後からITベンチャー企業の登場が国内でも盛んに見られるようになり（高柳，2009）学術的にも、日本ベンチャー学会をはじめとする、いわゆるスタートアップ研究やアントレプレナーシップ研究が盛んになってきたのもこの時期である。これらの多くは情報テクノロジーをプラットフォームとしているのである。その文脈において本論の副題にもなっている、ITベンチャー企業としての「エモスタ」の例も創業者へのインタビューなどをもとに論じて行きたい。さて、これらの歴史的背景を踏まえ、特に、近年のロンドンオリンピックと、2020 年に開催予定となっている東京オリンピックにおける、顔認証技術の、いわゆる「社会化」と「社会受容」（高柳，2016）について考えてみたいと思う。ITテクノロジーのコモディティー化と大衆化により、AI技術が一気に安くなり、GoogleやIBMそしてマイクロソフトなどが、非常に安い価格でそれぞれのAI技術を提供し始めた。同時に、IoT（Internet of Things）の進展により、IoTの本質である食指としてのセンサーからのデータ蓄積も一般化して、大手のSIerと言われる大資本のソフトウェア会社のみならず「街場」のSIerもこれにチャレンジし、そしてサービスや商品とし始めた。もっとも重要な要素として、ストレージが無料に近く安くなったため、センサーから時刻々と取得されるデータを、無尽蔵にためることが可能になったことも大きな意味をもつ。したがって、センサー（IoT経由で）からのクラウド上にたまったデータ、つまりビックデータを、これらのAIに分析させることが、容易になったことで、顔認証技術が進んだのである。そして顔認証を前提とした場合、センサーはカメラになる。カメラ技術も日進月歩で、解像度は無限に上がり続けている。動画でも 4K と 8K による実用放送がNHKでも開始され、個人もホーム

カメラでこのレベルの画像や動画を撮影できるようになった。そして、それらを広帯域な回線を通して、無尽蔵にクラウド上にアップロードしストックできる様になったのである。前述のエモスタはこういった時代に典型的に出現したITテクノロジーをベースとしたITベンチャー企業であると言える。また、AppleのiPhoneをはじめとするスマートフォンは、個人のデータへのアクセスを制限するため、高度でかつ安価な個人認証技術として「指紋認証」と「顔認証」を短期間で一気にサービス化した。特に、本論との関係でいうと、ApplePayの日本国内でのローンチに併せて登場したiPhoneXの発売で、Apple Face IDによる個人認証が一気に広がり、これらの技術はスマートフォンにおける個人認証のみならず、各種プラットフォームにおける電子決済のキッカーとしての役割を担う様になった。日々日々便利になる個人認証ではあるが、一方で、そういった技術による「監視社会」への誘導を指摘する声（キム，2011）も多く聞かれる様になってきた。特に、共謀罪たるテロ等準備罪などの議論で、国家権力が個人情報を大量に保管・分析することへの威嚇もそれである。当然ではあるが、民間企業がビックデータを扱えるということは同時に役所も同じことが実践できる。この問題における争点は、いわゆる「プライバシー」の議論と重なる。例えば、マイナンバーカードへの写真登録においても、これに抵抗する勢力が大勢いたのは周知の通りだ。国家権力が個人の顔写真のような個人情報を保管することへの威嚇の多くは「気持ち悪さ」に依拠している。

さて、したがって、本論において議論すべきことは、顔認証技術の「社会化」とその「社会受容」についてである。ビッグデータの第三者（つまり、ここでは大別して、国家権力と民間企業になるが）への提供に対して、私たち一般市民の解釈についての議論である。各種の法整備がゆっくりではあるが徐々に進む中、本論では、テクノロジーの社会受容の側面を強調しつつその問題点を明らかにしたいと思う。

1．顔認証技術を中心としたプライバシーの議論の「典型的な」先行研究

顔認証技術に対して違和感を唱える議論は比較的歴史が深い。例えば田島は「住基ネット」の導入がはじまった2000年代前半に顔認証技術がこれらに応用されることへの違和感を「監視社会の恐怖」として精力的に述べていた（田島，2006）。そもそもこの議論は顔認証技術の「社会化」以前の問題として住基ネット自体が違憲であるとする渡辺などの意見と併記されており（渡辺，2006）、しかし、そのいずれもは本論でいうところのビックデータの役所による保管・分析への批判であることは間違いない。この時期には、これらの違和感をもとにした顔認証技術を伴う役所の個人情報の保管と分析に関する一連のシステムの導入に対する反対運動や、裁判も多数おこっており、いわゆる国民総背番号制に対する2015年の金沢地裁の差し止め判断などは、その論拠とされている。

田島、斎藤らによるこれらの主張は極めて民主的な議論であると評価できるが、本論との関係においての争点である「便利さとのトレードオフ」や「社会コスト」の諸問題についての議論がほとんどされていないことへの筆者の疑問をここで呈した上で後述したい。

また、1990年代以降、インターネットが日本で市民権を得るのと同時に一般の市民やそれが属する民間企業も役所と同様に「セキュリティ」という目に見えない敵を相手にし始める。つまりこのカウンターパートとしてのセキュリティビジネスが大きくなるのである。シマンテックやマカフィーなどのコンシューマー向けのセキュリティーソフトウェア企業がそれである。時を同じくして上場企業を中心にした内部統制の中でも情報セキュリティーは重要な位置を占めるようにな

り国内においてはJSOXがそれに火をつけた。また、プライバシーの観点では個人情報保護法の制定と時期を同じくして総務省の外郭団体としてJIPDECが立ち上がり中小企業などの組織に対してもプライバシーマークの取得を促し、2000年代初頭の一般的な商取引においてもこの「認証」を持っているかどうかが重要な取引上のクレジットとなり始めた。無論、国際的にはISO、ISMSやBSIなどもこれと同じ文脈である。また技術的には、クレジットカード情報や決済が生じるネット取引においてSSL通信が標準化し、2018年には、米グーグルのウェブブラウザであるChromeにおいてSSL通信をしていないサイト（これはECサイトなどに限らない）への接続を原則として事実上できなくするなどのリードが行われ、これにより、ほとんど全てのインターネットサービスプロバイダーやデーターセンターなどが、SSLを標準実装するサービスに一年を要さずに切り替わっていくのである。

ところで重要なのは、その認証がどのような意味を持っているのかを社会的共通の理解にしているかという点である。例えばプライバシーマークの認可プロセスの最初は、当該認可を導入する企業の代表者の「トップインタビュー」から始まるが、実態は代表者はプライバシーマークの導入をサポートするコンサルティング会社が用意したシナリオを読んでるに過ぎない。審査機関もそのことを前提の質問にしているため、本質的な問題の理解を促すにはかなりの無理がある状態だ。さらに、技術的な問題、つまり先述したSSL通信一つとっても、内容を理解している被サービス者はどれくらいいるだろうか。ハッカーのケビン・ミトニックとロバート・バモシはこの点を指摘をしている（ケビン，ロバート，2018）。つまり、テクノロジーが「社会化」する際におこる「社会受容」において、テクノロジーの真実はほとんど理解されないまま、文脈としての受容が行われるのである（高柳，2016）。したがって規制当局とそのカウンターパートとしての民間企業のみが経済的に相互作用を起こすだけであって市民は置き去りになるのである。

さらにここにきて事態を複雑化させているのは、規制当局と民間企業というプレーヤー以外に一般市民というプレーヤーが直接問題に巻き込まれる事態が多発していることである。特に、SNSの登場により、誹謗中傷や恐喝、そして場合によっては殺人にまで（これは極稀であり統計的には無意味であると思われるが）発展する事件の類いである。このことについて弁護士の山岡は一個人が民間企業を攻撃して当該企業のレピュテーションを大きく低下させる問題についてリスクマネジメントの側面からの論考を続けており（山岡，2018）、同時に、民事と刑事においてこの問題の解決に司法の場で挑んでいる。同時に3番目のプレーヤーとしての一般市民は、属する組織によりこれら「セキュリティ」への理解を少しでも深めることが当面の課題となっていることも指摘している。山岡は、攻撃者が極めて高い匿名性を持っているのに対し、被害者の「顔」が判明していることを指摘しており、確かに、公権力のみならず、個人情報としての「顔」のデータが何らかの形でネットに流出することに警鐘を鳴らしている。

また念の為ここで触れておくが、私たち一般市民は、日常の情報行動や経済活動の中でも「監視」されているのは周知の通りである。パリサーはAmazonやGoogleにおいて私たち個人の行動履歴や趣味志向、そして、場合によっては位置情報までを含む個人情報がターゲットマーケティングの属性になっていることを「フィルターバブル」と表現して説明（パリサー，2016）しているし、同じようにブルースもまたパーソナライズド広告という表現を用いて個人の一挙手一投足に及ぶまでがビジネスの対象になっており、同時に、民間企業と権力との連携によってこれらのビックデータが保持されることで監視社会化しているこ

とに警鐘を鳴らしている（ブルース，2016）。なお、ケビンとロバートやブルースの論評が重要な理由は、前者はハッカーであり、後者はコンピュータセキュリティの権威で暗号研究者だからである。前述してきたように、第3のプレーヤーである一般市民が置き去りにされるのは、テクノロジーの解釈、つまり技術論を忘却した状態で議論に巻き込まれるからである。ここに記してきた先行研究はいずれも「警鐘」という意味では同じ方向を向いていると言える。しかし田島の指摘にはソリューション（解決策）や代替案が含まれない。ここが筆者が近年指摘している後述する「テック・リテラシー」の不足による議論の無意味化なのである。一方の技術者による論評の多くは必ず問題の根本が何であるかを技術的具体的に指摘した上でソリューションを提示している。この違いが技術の「社会化」においてどれだけ重要なことかを最初に指摘しておく。そして、これらの問題は決して社会科学の中だけで論じられることではなく、工学を含む学際領域での議論が必須であることはこれまでに指摘してきた通りである（高柳，2016）。

2.「便利とのトレードオフ」とは何か

次に顔認証技術の実装について述べておく。多くは既に「社会化」しており「社会受容」の過程も極めてスピーディーに進んだ。

まずはAppleのスマートフォンであるiPhoneのiPhoneXで実装された顔認証システムの「Face ID」である。当該機種は2017年9月12日に米国カリフォルニアで発表されて翌10月27日から予約販売がスタートした。この機種から搭載されたFace IDはスマートフォンにアクセスする際のロック解除や、ApplePayにてオンサイトとオフサイトの両方で決済する際のキッカーにも使われた。またサードパーティーにもAPIを公開していることからサードバーティーが開発するアプリへのアクセスや何らかの個人認証の際に利用することができる。例えばヤマト運輸の公式アプリには当初よりこの機能が実装されているが、詳細は後述するとして主な実装理由は強固なセキュリティーよりも上質なUI（User Iuterface）によるUX（User eXperience）を提供するためである。つまり、アプリの利用促進のために用いられ、いわゆる複雑なパスワードのタイピングストレスによる「離脱」を防ぐのがその主要な理由である。念の為、技術的な概要をAppleが公開している範囲での技術仕様から引用すれば3万ドット以上の赤外線を顔に照射しそれをiPhoneXに装備されているカメラ（赤外線カメラ）で撮影することにより一時的に3Dモデリングを行い過去に登録した顔データと照合するもので他人がロックを解除できる可能性は100万分の1程度であると発表されている。ちなみに、それまでのiPhoneが実装していた指紋認証システム（Touch ID）の精度は5万分の1程度とされており20倍の精度となっている。

次により身近な例も示しておく。セブン＆アイ・ホールディングスの中核子会社でコンビニエンスストアのセブンイレブンを展開するセブンイレブン・ジャパンは2018年12月18日、スマートフォンなどを一切用いずに顧客の顔認証だけによって無人店舗で買い物ができる「顔パス」コンビニをNECと共同で運用することを発表[1)]した。試験店舗は東京都港区のビル内にある店舗である。小さな店舗で約400点の商品を販売するが先に登録されている「顔」データと会計の際にレジのカメラで読み取った「顔」データの照合をはかり個人に紐づいた決済手段から決済を行う仕組みである。コンビニの場合は顧客満足の一方で、人手不足による業務の合理化が急務でありそのための無人レジへの投資は同社だけでなく他社においても長く行われてきている。私たちの日常生活に根付いたという点においては貴重なサンプルである。

さて、ここでの争点は、利用者が例えばコンビニでFaceIDなどの顔認証技術により、または、このセブンイレブンの事例の様に、顔を撮影させて決済をすることに対しての違和感の有無である。国内の電子決済プラットフォームは述べるまでもなく、クレジットカード系と交通系の2つに大別される。前者は商標で言えばクイックペイやIDとなり、後者はSuicaやPasmoに代表される。これに続いて、非決済系プラットフォーム事業者も抱えるユーザー数を利用し電子決済に参入しており、Origami PayやLINE Pay、ソフトバンクグループのPayPayなどが有名だが、2018年は日本における電子決済プラットフォームの争奪戦元年と言える。何れにせよ、コンビニなどの小売店では現金以外での決済手段としてクレジットカードに続きこれらの電子決済が重要な鍵となっており、利用者数は短期的にそして急激に増えつつある。

ところで、前述してきた様に、マイナンバーカードへの顔写真の提供の際には、大きな問題になった。これは提供をする先が役所であることが一義的にはあるのと、納税に直接的に関係する事例だったからという仮説も成り立つ。しかし、小売店での電子決済において、顔認証などの個人情報の民間業者への提供について、これまで大きな反対活動は起こっていない。筆者はその理由の仮説としてここでは「便利さとのトレードオフ」をあげる。国民全員がスマートフォンを持つ中でキャッシュを利用せずに日常の決済が完了することは、そのそれぞれの個人が個人情報たる「顔」データを毎日何度も何度も民間企業に提供する違和感よりも圧倒的に優っているからではないだろうか。念の為付け加えると、AppleのFaceIDは顔認証を行う際、前述の公式発表に寄れば、毎回の顔データはクラウド側に送信せず、スマートフォンのローカル側に入ってるCPUたるチップ（iPhoneXの場合はA11チップ）内に保存し問い合わせを行ってるとしており、見方によっては、クラウドでのビックデータ化は行っていないためプライバシーに配慮しているとも読み取れる。またエストニアの「電子政府」（前田，2016）（武邑他，2018）は極端な例としてここ数年着目されてきたがヨーロッパの小国の生き残り策としてとはいえ、こういった「eガバメント」的なプラットフォームが社会実験として成り立った場合、総務省のマイナンバーロードマップのレベルをはるかに超える「便利さとのトレードオフ」の実例が公共セクターに出てくる可能性も多分にあるのである。

また顔認証技術だけのことではない。ひと世代前の指紋認証技術についても同じことが言える。指紋については議論は長く、古くは1955年に制定された指紋押捺制度に遡ることができる。つまり身体的にユニークな特徴である指紋を用いて個人を特定する（個人認証する）ために、主に、外国人登録元票に使われてきた一連の歴史である。これは旧外国人登録法14条に端を発する議論である。差別に繋がる指紋による個人認証は外国人の人権について大きな議論[2)]を巻き起こしたきたが、これと呼応するかたちで交通違反切符に対する運転手への指紋押捺強制についても議論が大きくなったこともある。これは切符を承認する際に押印を求められるが多くの運転手は印鑑を持参していないためその代替え手段として指紋の押捺を強く警察側に求められることへの違和感から不満が噴出した例である。法令では指紋押捺は強制ではなく任意であるため、現在ではこれを拒否してその代わりにサインをすることができる様になっている。つまり、指紋押捺については長年の様々な偏見やそれを克服するための議論によってその行為自体に意味付けがされており、一般市民においても押捺への拒絶感が強いことが理解できる。

しかしである。Appleという（あるいはApple以外のスマホメーカーも）いち民間企業が、1日に何回も何回も個人認証のために「指紋押捺」を

求めることは、何ら議論にならないし、ましてや大きな反対運動もおこらない。何もスマートフォンに限ったことではない。「セキュリティ」への対策として各種認証を守るため民間企業がPCへのログイン技術として安価な指紋認証を導入しても、これに不服を唱える活動は起こらないのである。ちなみに、TouchIDもFaceIDと同様にローカル側に参照元となる指紋データを保管し、そこへ照合しているためにクラウドでのビックデータ化は行われていないとメーカーは発表をしている。

さて、ここまで述べて、もう一度「便利さとのトレードオフ」の争点について考えてみたい。つまり顔認証も指紋認証も社会受容される際に、利用者にとって圧倒的に優位性があった場合、つまり、便利だった場合に、それに反対する議論が起こらないことが想定される。住基ネットにせよマイナンバーにせよ、外国人登録証にせよ交通違反切符にせよ、それは個人認証をされる側にとって何ら一義的なメリットはない。よって、総務省が目下横串で展開している「マイナンバーカード利活用推進ロードマップ」は徴税目的だけではなく免許証や保険証などもこれと一体にすることで便利にし、そんな反対を封じ込める役割があると理解できる。一方で、提供先が民間か役所かという議論も散見されるが、それについては次の章でさらに深めたいが、何れにせよ、これをこの争点の一旦の仮説としておく。

3. 民間セクターと公共セクター、上場企業としてのGoogleの限界

これまで述べてきた様に民間セクターによる情報収集と公共セクターによる情報収集については、私たちが抱く印象（その多くは確定的なものではなく「気持ち悪さ」であるが）が大きく違う様だ。公共セクターに対する特に個人情報の収集に対する反発については田島らによる主張の通りであるが、それでは民間セクターにおける情報収集についてはどうか。前章では「便利さとのトレードオフ」であろうと言う仮説を設定したが、一体どの時点で「便利」と判定できるのかと言うことも考えないといけない。

この点についてはイノベーション論の基礎を援用するのが一般的だと考える。つまりテクノロジーの「社会化」の過程が、どんなに素晴らしいテクノロジーであってもスムースに進まないことは筆者が述べてきた通り（高柳，2008）であるが、シュンペーターのイノベーション普及学を基礎とするムーアの「キャズム理論」（ムーア，2002）によれば、アーリーアダプターとアーリーマジョリティの間に存在するキャズムを超えるタイミングが一般的に「便利」と言う認識と重なると解釈される。つまりAppleのiPhoneXを例にとれば顔認証たるFaceIDが実装されたのはiPhoneXからであるから国内における現在の出荷台数に対してい「キャズム理論」のイノベーターとアーリーアダプターを足して16.0%を乗じた出荷台数が「いつ」達成されたのかを計算すれば良いだけである。なお、国内に絞ったiPhoneXの出荷台数をつぶさに分析することは困難を極めるがApple社の決算発表資料（10-K）を元に調査会社のCounterpointが分析した数値[3)]を参考にするとiPhoneXの出荷台数は2018年10月までに積算で6300万台に達している。つまりその時点でのキャズム周辺は1000万台強であるため同資料による発売から10ヶ月の積算推移に照らすと発売日からたった2ヶ月から3ヶ月目の間に達成されているのである。

つまりAppleにおけるFaceIDが便利だという共通認識が構築されたのが2017年の年末頃だったと言うことが言える。つまり急激なスピードで市民が「便利」を享受されたことになる。念の為指摘すると顔認証技術による個人認証についてはAppleだけが取り組んだ訳ではなく、他のスマートフォンメーカーも同じ頃（またはその少し前）

に実装をしているが、ここでは便宜的にAppleの事例を利用する。またECでの決済やコンビニなどの店舗での決済時のみならず、そもそもスマートフォンにアクセスする度にFaceIDによる個人認証が必要な訳で―これはTouchIDでも同様だが―まさにこの情報行動自体は日常そのものである。しかし、これだけ短期間にいわゆる市民権を得て、そして、どこに行ってもこの情報行動を「強要」されるにも関わらず、FaceIDについてプライバシーや監視社会の観点でAppleを相手取った訴訟や抗議活動が大きく展開され社会現象化した事例はないのである。また、前述した通り、Appleの公式発表においては、元となる顔写真のデータはローカルのチップの中に保存してクラウドには送信、保管しないことを「わざわざ」その仕様の中で明記している。つまり当然であるが事前にこの技術への一定の反論に対しての予防線を張った形になる。無論、通信が途絶えている間にもこの機能は確実に使えなくてはならないためローカルに保存する必要はあるが、一日多数回行われる顔写真の事実上の取得データをローカルからクラウドに送信することは事後であっても容易い。その形跡があるかないかについての第三者機関による解析は今の所されていない。しかし、それもそのはずで、私たちは「便利さとのトレードオフ」で無意識に顔データや指紋を大量に民間企業に取られていることに対する「違和感」すら感じなくなっているのである。あるいは感じていたとしても反対活動や不買運動として表出するまでにはなっていないのである。

前章で述べた通りであるならば役所が行う個人情報収集についても、その「対価」として圧倒的な「便利さ」を提供すれば反対運動は起こらない可能性が示唆できる。つまり総務省の一連のマイナンバーカードの利用促進プロジェクトがそれに当たるが、一方で、公権力の側が、仮に善意の行動であっても個人情報を収集保管することへの反発は免れないとするのが一般的である。では、民間企業であったら安心なのであろうか。

これまでにもGoogleが中国政府の要請に応じて中国政府を批判するアクティビストが利用しているGmailのデータを当局に渡したことにより当該アクティビストが中国当局に拘束されると言う事件が続いてきた。これはGoogleだけに言えることではなく、メールサービスを提供する企業全体に共通することであるが、そのシェアからしてGoogleが目立っている。またその度にGoogleの担当責任者が米国議会に招聘されてきた。[4] しかしなぜこう行ったことが起こるかと言えば、そこにはクラウドドミナントのGoogleだからこその問題も垣間見られる。

つまり現在中国では米系の多くのサービスはグレートファイアウォールにより規制されている。当然Googleの各種サービスも中国国内のインターネットにおいては使うことができない。ただし、一般市民レベルでは「違法」のVPNサービスを利用して米系のサービスを使うのが一般的ではあるが、しかし、誰もがこれを利用しているわけではない。西側諸国の旅行者も同様で宿泊するホテルにおいてもインターネットに接続する際には米系サービスへ接続できないことや閲覧内容などが当局により検閲されていることへの注意喚起がされれている。一方で、Googleにしてみれば、13億人とも14億人とも言われるマーケットを制することが次の成長になる。同社の前CEOであるシュミットが足しげく北朝鮮に通っているのは同社のOSを搭載したノートパソコンを教育支援の名目で無償提供していると言う報道も多くある。[5] 現在ChromeOSのシェアはWindows、Mac、Linuxに続いて4位である。これの拡大も重要なマーケティングである。同様に中国において同社の数あるクラウドサービスを解禁させることは悲願以外の何者でもない。したがってそのバーターとして中国政府の要請に対し「柔軟に対応してしまう」ことも容易に考えられる。当然であるがこ

の背景には株主資本主義がある。上場企業たるGoogle―実際はその持株会社のAlphabetが上場しているが便宜的にこのような表現とする―はまず第一に何を捨てても株主に貢献する責務がある。これまで積極的なM&Aでドミナントの地位を獲得してきたのは高い株価に裏打ちされたマーケットでの天文学的な調達能力があってこそであると言うことは自明である。

ところでGoogleは上場企業として未上場企業と異なり高い透明性と一定の公共性が求められる。その文脈から事実上のドミナントとしての社会的責任論も散見される。しかし株主資本主義において、透明性と言うのは、あくまでも株主や潜在的株主への透明性に他ならない。無論ステークホルダーの中には消費者、つまり、この文脈においては中国当局に拘束されたアクティビストも入るのであるが、しかし、特に米国型キャピタリズム（または金融資本主義）においては、それをもってしても株主への還元が優先される。これが性善説的な上場企業の、または、株式会社としての責務と要請を纏ったGoogleの限界と考えるべきなのである。したがって、上場マーケットの規制当局であるSECなどの興味はこの点について極めて薄い。

さて話を戻すが個人を認証するための顔データや指紋データに代表される個人情報の公共セクターや民間セクターへの提供について、民間セクターへの提供の方が「便利さとのトレードオフ」によって「スムーズ」に行われる事象について述べてきたが、しかし、一方で、その両方が最終的に行き着く個人の情報の扱い方についての危険はいずれも同等程度に存在するのではないか、と言う点が本章で一旦押さえておきたい結論である。

4. アメリカなるものに対する違和感、GDPRの制定

いわゆる「the Internet」は民主的で純粋なテクノロジーとして語られることが多いが、しかし筆者は長いことその実態は極めて政治的でアメリカなるテクノロジーであり、アメリカ優位の経済社会を構築する有望なツールであるとこれまでも繰り返し述べてきた（高柳，2010）（高柳，2014）。クラウド優位のビックデータの時代に差し掛かり、それはさらに顕著に現れている。その一例がEUによるGDPR（General Data Protection Regulation：EU一般データ保護規則）の制定である。これはEUに在住する市民の個人情報の取得に対する規制であり、国内の個人情報保護関連法に裏付けされるプライバシーマーク制度に実務的には似ている。法律の内容自体の詳細にここで紙幅を割くことは避けるが、これはEU国内のみならず、むしろ米国をはじめとするEUの外の企業活動に大きな影響を与えるものになっている。また罰則の厳しさも一つの特徴となっており、その制裁金は違反の内容によって異なるが「最大で企業の全世界の売上高（年間）の2%、または1,000万ユーロのうちいずれか高い方」や「最大で企業の全世界の売上高（年間）の4%、または2,000万ユーロのうちいずれか高い方」と、とてつもなく巨額の制裁金となっている。またEU以外の企業の場合はEUに子会社、支店、営業所を有している企業、となっており、日本国内でのみ営業をしている企業は「事実上」除外されるようにも読めるが当該企業がEU内に何らかの資産を持っている場合に差し押さえの対象になることも考えられる。これにより日本国内においては高いコンプライアンスを求められる上場企業を中心に未上場の中小企業までネットで英語などの多言語サービスを行なっている企業はこぞって「GDPR対応」を自社が展開するECサイトなどのWebサービスで行い、SIerの間ではGDPR特需などとも呼ばれた。また実際、2018年7月にはホテルのブッキング

サイトである「ファストブッキング」のサーバーが不正アクセスを受けて個人情報の流出が判明し、ここに業務を委託しているプリンスホテルや藤田観光などの日本の大手企業がGDPRの最初のターゲットとなった。[6] このGDPRの精神はEUの在住者の個人情報を主に民間ファクターから守ることが最前提となっており、特に、ターゲットマーケティングに資するようなクッキーの取得をはじめとするネット上での行動履歴のマーケティング活用について厳しく言及されている。つまり、GAFAをはじめとする米系ITサービス企業のビックデータ活用を牽制していることは明白である。これはインターネットの初期にヨーロッパーが「アメリカなるもの」としてのTCP/IPの受け入れに何色を示した行動に酷似している（高柳, 2010）。特にフランスは最後まで自国の国営電話会社が推し進めていた「ミニテル」の優位をうたいTCP/IPを拒否し続けたが結果は周知の通りデファクト・スタンダートしてのTCP/IPがヨーロッパにもインフラとして存在することとなった。このように、主にGoogleを含むGAFAの対立軸として中国が注目される中において、ヨーロッパとアメリカの対立軸も検討することは極めて重要である。

またクラウドサービス企業（ソフトウェア企業）がこの問題でクローズアップされるが、本来は人々の情報行動履歴をリアルタイムで取得するセンサーのアッセンブリーとしてのIoT企業（ハードウェア企業）にもっとも注目をしなくてはならない。例えば、EU在住者やアメリカ在住者、そして日本在住者などが交差すると思われる交通やリゾートなどの産業もこれらの問題に直面している。

オーストリアに本拠をおくSKIDATA社はスキーリゾートのリフト改札などでグローバルで大きなシェアを持っているが、その最新のリフト改札には改札を通過する人の顔を全量撮影保存するためのカメラがついている。これは一義的には不正な改札通過をなくすため、導入企業に貢献するわけだが、しかし、当然これらの「メカ」はクラウドに繋がっており、そのデータはデジタルマーケティングにも活用される。むしろそちらの方が大きなインパクトがある。となれば日本国内においてもこのハードウェアとしての改札を導入する企業はインバウンド需要も考えればGDPR対応をし、そして、来場者の顔データは一体誰がどのように二次利用できるのかについてリーガリーに整理して理解する必要があるのだ。しかしこれはなかなか大きな経済コストとなる。

またGDPRの議論で重要なのは、これまで何度も指摘してきたような「便利さとのトレードオフ」である。あるプレーヤーにとって「大きな経済コスト」であっても、それを超えた利益がもたらされ、一方の個人情報提供者の情報行動にも資するものであれば提供者と管理者（GDPRの文脈ではコントローラーと呼ばれる）の間にコンフリクトは生じにくい。SKIDATA社の例をとれば、個人情報の二次利用によりロイヤルカスタマーに次の来場の際の割引クーポンを発行するなどの付加価値がそれに当たる。そうなった場合、個人情報提供者は「喜んで」個人情報や顔データを提供することが考えられる。少なくてもAppleのFaceIDにおいてはその状況は確定的に存在した。このトレードオフの議論は田島の議論では全く抜け落ちているのである。また、この抜け落ちていた議論については、後述するデジタルネイティブの特性理解においては極めて重要な争点になるのである。

ところで、EUはGDPRで事実上GAFAなどに対して牽制をしているのであるがその一方で、それとは真逆の事例も出始めている。例えば、EU特許庁（EPO：Europian Patent Office）は2012年にEUにおける特許業務の特徴である複数国語への翻訳業務をGoogleの自動翻訳に限り許可する声明を発表[7] しているのである。極めて大き

な負担となっているEUの翻訳業務において自動化の入札を行った結果Googleが落札したのだが、翻訳を担うということは膨大な特許の全ての情報をGoogleが保存可能な状態になる。これについてEUの特許実務を行うアトーニーが集まるブログでは様々な意見が交換されているがその多く[8]に共通するのは強い違和感である。そもそも民間企業のGoogleが知的財産に関する情報―当然だがそれらはビックデータ化される訳だが―を役所が知財として登録する前に知る事へのアトーニーたちの依頼人に対する不利益や、検索のドミナントであるGoogleがその特許情報の検討に関する行動履歴を同時に収集する可能性へのプライバシーの問題などがそれである。これまでのヨーロッパによる「アメリカなるもの」への抵抗や違和感の提示とは真逆の役所によるGoogle導入の決裁プロセスであるが、財政悪化に伴う唯一の解決策としてのGoogleであったことは否めない。まさにGDPRを制定した地域で、それとは全く逆のことが、つまりEU在住者の個人情報を含む権利や知財、そしてプライバシーに纏わる情報を進んでGoogleに提供しているのである。これもまた究極の「便利さとのトレードオフ」であり、このトレードオフが生活者個人だけに起こるものではなく、国家においても適応されることの実例として押さえておきたい。

5. 文化装置としてのオリンピックと顔認証技術

近代オリンピックが文化装置であり、特に1980年代以降においてのそれは、いわゆるメディア・イベントであるという点について多くの研究がある。筆者もメディア・テクノロジーの社会化のプロセスにおける宮内庁による天皇陛下の「天覧」がメディア・テクノロジーのその後の「社会受容」を短期間に達成することに繋がったことについてこれまでも言及してきた（高柳, 2010）。顔認証技術の文脈において文化装置としてのオリンピックが注目されたのは2012年のロンドンオリンピックである。テロを未然に防ぐ、または、テロへの不安を払拭するためロンドン市内を中心に大量の監視カメラを設置したことから始まる。当然ながら日本国内の企業もこれに主体的に参加しており、パナソニックは公式スポンサーであると同時にすべての会場の周辺に同社のセキュリティカメラ（セキュリティCCTV）を設置し、その総数は2500台以上に及んだ。当然ながらセンサーとしてのカメラ単体を提供したのではなく「高度なセキュリティーシステム」[9]を全体としてソリューション提供しておりその中には個人を識別する顔認識技術も含まれている。またパナソニックは現在、その実績をもって同社独自の顔認証技術を利用したディープラーニング顔認証システムを「FacePRO」[10]という商標で積極的に展開している。イギリス国内には2008年時点で約423万台もの監視カメラが設置されている。ロンドンオリンピックを遡ること7年、2005年7月7日に発生したロンドン同時爆破事件などに端を発し「防犯」の意味合いで導入が進んだ。1990年代には個人のプライバシーを侵害するという論拠により大きな反対運動が起こっていたが、1993年に発生した幼児殺害事件であるジェムズ・バルガー事件において当時の防犯カメラがその解決に大きな役割を果たしたことが報じられて以降、また加えて1998年に犯罪及び秩序違反法が制定されたことも加わり大きな公共投資が可能となりセキュリティーカメラの導入が急激に進んだ都市の代表となったのである。

翻って2020年に開催が予定されている東京オリンピックでもテロの抑止などを目的に監視カメラの整備が進められている。直接的に当該イベントの公的な入札に関わるものや、入札以外の一般的な商取引においてマーケットが加熱することも予想されることから、監視カメラの製造や導入を行う上場企業の株式は注目されている。監視カメラメーカー（製造）の大手銘柄では、日立製作所、

NTT、富士通、JVCケンウッド、NEC、パナソニック、ソニー、キャノンなどの名前が連なるが、IPベースの監視カメラをソリューションとして提供する高千穂交易やカメラで撮影したデータを録画する専用サーバーを構築、運用するビーマップ、そして交通機関に特化した監視カメラを提供するサクサホールディングスなど中小ベンチャー勢も注目を浴びている。パナソニックはロンドンオリンピックに続き東京オリンピックでもワールドワイドTOPパートナーを引き受けたこともあり、ロンドンオリンピック後の2014年からグローバルベースのセキュリティーシステムの企業や映像システムなどの会社の買収を続けていた。また上述した内、国内ゴールドパートナーはNEC、キャノン、NTT、富士通であり、それぞれ、NECは先進セキュリティカメラ、キャノンはレンズやスチルカメラの経験を生かしながら監視カメラ世界最大手のアクシスの買収を2015年に発表し、NTTは通信サービスを、富士通はデータセンターを提供することになっている。これ以外にもJR東日本は2018年春以降に山手線内への防犯カメラの設置を行ったりと巨大マーケットを前に活況である。

また周知の通りこれらの監視カメラの設置の裏付けとしてはテロの防止を筆頭とする脅威への対策があげられる。法整備もいわゆるテロ対策特別措置法をはじめテロ等準備罪が内閣より提出され施行されたのは記憶に新しい。国会での侃々諤々の議論と並行して市民生活の中においても防犯カメラやドライブレコーダーの映像分析による事件解決は日々マスメディアを通して報道され、2018年のハロウィンには渋谷区のセンター街で軽トラックを横転させ暴徒化した若者たちがその上で騒ぎ立て、のちに、周辺の防犯カメラの映像と、容疑者たちが自宅に帰るまでの防犯カメラの映像を利用して警察がすべての関係者を短期間に逮捕するに至ったことが大々的に報道された。警視庁捜査1課が現場周辺の約250台の防犯カメラの映像を分析したというのが公式な当局発表である。同様にドライブレコーダーの映像による事件解決は膨大な量に達し、JEITA（電子情報技術産業協会）の発表[11]によれば、ドライブレコーダーの出荷台数は2016年度の1,456,829台に対し、翌2017年度は2,665,309台に達し、2018年度に至ってはなんと上半期だけで1,651,075台に達する急激な伸びを示している。このように、テロや注目事件を契機に、少しずつはじまる監視カメラの導入は、その社会的ソリューションとしての成果をマスメディアがアナウンスすることでさらに日常生活の中での導入が前提となり、それを合法化する法律が制定されることで一気に一般化して賛否の議論が下火になるのである。当然その中において監視カメラに纏わるサービスは拡大の一途をだどるのである。つまりこれらの事例からもわかるように、いわゆる、メディア・イベントによって、あるいは「天覧」のような権威づけを受けた個人認証技術は、その反対議論をものともせずに「社会受容」に至るわけだが、これもまた「便利さとのトレードオフ」そのものなのである。

6. 顔データの分析を行う企業の意識―株式会社エモスタ[12]とその創業者たちの事例―

近年、デジタルカメラの解像度が飛躍的に上がり、一方でそれらのデータを保管しておくクラウドストレージがコモディティー化したことを受けて、画像や動画の認識を行うAIの開発が急激に進んでいる。大手のベンダーではIBMがWatsonを、マイクロソフトがCognitive Servicesを、SalesforceがEinsteinを、そしてGoogleがCloud Vision APIをとそれぞれの強みを生かして無料をベースに有料でも安価にAPIにより提供しており誰でも使えるようになっている。その中でこれらの領域に小資本のベンチャー企業も進出しており、今回取り上げるエモスタもその内の1社である。

エモスタは感情認識AIを開発、サービス提供を行っており顔の動画や画像からその人の感情を高精度で読み取るといったユニークなテクノロジーを提供している。創業者は2名でCo-FounderでCTOのAlexander Kriegは米国において心理学の博士号の学位を取得した学者であり現在、日本で私立大学の教員職に就いている。またCo-Founderで代表取締役を務める小川修平は米国の大学でスポーツマネジメントを習得後、大手投資銀行勤務を経て同社をKriegと共に創業している。両者とも特にコンピュータサイエンスのバックグラウンドは無く、Kreigがコードを書ける程度であるが、心理学のバックグラウンドと金融のバックグランドをもって感情認識AIのベンチャー企業をはじめるることができたのいうのは前述したようなITがコモディティとなった時代を象徴している。特徴的なのは創業者の2人を見る限り他のテックベンチャーの様にコンピュータサイエンスの経験に依拠していない点であり、同時に、Kreigが心理学者であるという点だ。ここではエモスタの企業分析は行わず、本論の文脈において2人のインタビューを引用しながらこれまでに議論との関連を示してみたい。

そもそも表情から感情を読み取る感情認識AIに対する消費者のニーズの多くは「人の本心が知りたい」というものだと小川はいう。なお、この「本心」には嘘が含まれるという点が興味深い。具体的な導入シーンの一例としては保険の申し込みおよび申請などである。近年、営業人員のスキルに依存する対面契約ではなく、ネットでの契約が進む保険営業において、契約対象者の顔データをスマホやパソコンに搭載されているインカメラで撮影しながら契約または申請行為を行うことにより、契約・申告内容の真偽をAIが判定するというものだ。あるいは次に多い導入シーンとしては人材サービスなどの人材の面談のシーンだという。いずれも、いわゆる「本音と建前の本音が知りたいとき」にエモスタのサービスは有効であるという。これらは当然、記入や発言内容が事実であり詐称が無いかについてAIが人間に助言をすることになる。

ただし、大きな課題として、そもそもAIかどうかに限らず嘘と真実の境の認識が難しいという問題もあるという。当然であるが人すら相手の嘘を見抜く力、または、真実を見抜く力の基準は無く、したがって、AIが参照すべき「教師データ（ビックデータ）」作りにかなりの時間とコスト、そして経験が必要になるのである。なお、人による一般的な表情を使った嘘の発見確率というのは特殊なラボの中であっても55%程度ということで優位性は無いのが現実だ。

また重要な点として多くのAIはビックデータを参照することでその精度を上げていくが、ビックデータは過去のデータであることが多い。当然、将来のデータを大量に蓄積することは不可能である。例えば、2018年10月10日にロイターが伝えた報道では、米アマゾン・ドット・コムは、それまで行ってきたAIによる人材採用オペレーションを中断したが、その理由がAIが女性を差別する採用をしていたことが明らかになったからなのだという。なぜこのようなことが起こるかといえば、男性優位の採用をしてきた過去のビックデータがすでにバイアスを含んでおり、それをAIが参照したからだと分析されている。このように、ビックデータたる教師データを参照したAIの判断は必ずしも人々の将来の社会に完全に適合しているとは限らないためエモスタにおいてもそのAIが弾き出す結果はあくまでも参考として活用される事例が多い。

ところでこれまでGDPRや個人情報保護法などの章でも述べてきた通り、これらの議論の中には3者のプレイヤーがいる。1つはサービス提供者である。エモスタがこれにあたる。次に監視者

（コントローラー）であり、この文脈ではエモスタを導入し、それを利用してエモスタが弾き出す結果を利用するプレーヤーである。そして３つ目は被監視者であり、エモスタによって分析されれ、その結果を活用されるプレーヤーだ。

結果としてエモスタが導入された場合の多くが、この監視者と被監視者の関係が「世界観の合意を強制できる」シチュエーションであったという。別の言い方をすると等価交換が成り立つ関係だったとも小川は表現する。具体的にはカウンセリングがこれにあたる。カウンセラーと患者の関係においてエモスタが介入することでより科学的客観的に患者の状況をカウンセラーが把握でき、その結果、エモスタが介入しないときよりもより良いサービスを患者に提供できる関係であり、カウンセラーも患者も満足度が高い状況である。つまりカウンセリングという行為の約束自体が「世界観の合意を強制した」と言える。同様に医師のインフォームドコンセントのニーズも多いという。専門家たる医師が患者に対して顧客満足を提供できるとは限らない。そのため、患者の表情データからリアルタイムに感情を抽出し、医師に対して患者の反応を科学的に伝えることで医者のインフォームドコンセントが的確になり患者の顧客満足度が上がり、両者の間に等価交換が完了するということだ。

つまり「世界観の合意を強制できる」状況というのは、これまで述べてきた「便利さとのトレードオフ」と同義である。被監視者の持つ個人情報の価値よりも、それを監視者に提供した時に得られるリフレクションの価値の方が大きいときに被監視者は喜んでこれを提供するのである。したがって、iPhoneXのFaceIDの「社会受容」と同様の理屈なのだ。

ところでこの「世界観の合意を強制できる」状況が進むとどのような社会状況になるかを小川に聞いたところ「（等価）交換のグラデーションが作られる」という答えが返ってきた。つまり、自治体単位で「個人情報を完全に提供する代わりに税金がゼロの自治体」から「個人情報を全く提供しない代わりに税金が高い自治体」までのグラデーションがある社会になるという意味である。そこに住む市民は自分の好みで自治体が選べる。

前出のエストニアの事例は当時非常にセンセーショナルに伝えられたが、日本と比べると圧倒的に小さな国である。したがって、なかなか１億人を超える民主主義国家で資本主義を導入している成熟社会にこれを適応するは難しい。しかし、自治体レベルであれば可能性は高い。現に公共サービスの負担軽減の為のIT化は全国で起こっている現象である。その意味で小川の主張は興味深い。

また顔データと感情データについては、それぞれを分離することは可能であり、顔データは現行法下でも個人情報として確定しているが、顔データと分離した感情データは法的に個人情報かどうかは未確定であるという。またさらに、感情データから個人情報を技術的に抜き出せるかどうかについても判例はもちろん学術的な研究も進んでいない。何れにせよ、遵法性の観点からビジネスのプラットフォームで活用する場合はプライバシーが及ぶ領域として扱うしかないというのが現状だ。その上で、小川は、個人情報保護やEUのGDPRの文脈で言えば、当該情報（つまり個人を特定できるような情報）を監視者に提供しないことが逆に危険なのではないかと指摘した。つまりこれだけ大量の個人情報がビックデータとして管理される状況において、その時間にどこで何をしていたかを常時提供しないと「アリバイ」が成立しないため危険だという意味である。これを小川は今の個人情報保護またはプライバシー保護方向の社会の潮流に対し「逆回転」と表現している。

小川は1986年生まれ、Kreigは1990年生まれ

である。冒頭に触れたデジタルネイティブは1995年以降に生まれた世代と定義しているので、それらとは5年強ほど離れている。しかし、個人を特定するための顔を含む情報の民間セクターや公共セクターへの提供についての考え方が戦後すぐに生まれた世代とは明らかに異なっていることについて私たちは理解を深めなければならない。またデジタルネイティブと言っても、近年のクラウド化のスピードや、それに伴うターゲットマーケティングの急激な発達、そして、それにアジャストする「便利さとのトレードオフ」の感覚についてもアップデートしながら議論を進めないといけないのではないだろうか。

おわりに

本論の主軸は結局のところ「ビックデータ」である。ITのコモディティー化がもたらしたこれまでとは単位も規模も異なるデータの塊の中には、私たち生活者の行動履歴の全てが含まれることがある。また、それ以外に、趣味嗜好といった極めてプライベートな情報も内包され、それがデジタルマーケティングに生かされている。それによって「テレビ時代」にはCM中にトイレに行くことが当たり前の行動であったが、そもそも、能動的に見ているコンテンツよりも興味を抱く「CM」が目の前に出現することにより、全てのコンテンツが興味の対象となり、つまり「リマーケティング」されることが当たり前となった。特に「テレビ時代」を知らないデジタルネイティブにとっては、文字通りそれは「当たり前」なのである。加えて、実例として取り上げたエモスタの様に、行動履歴や趣味嗜好だけではなく、私たちが無意識のうちに表出している表情やそれに関連する感情までもがビックデータ化する社会において、一体、個人情報やプライバシーの概念はどうあるべきなのかを、あくまでも社会学的に整理しようというのが本論の狙いであった。

同時に個人を特定する技術としての個人認証の技術が進んだ。今までは「4digits」を入力することでログインしていたが、生体認証としての指紋認証に続き、その20倍以上の精度を誇ると同時に極めて便利で負担が少ない顔認証技術がスマートフォンに実装されるやいなや、公共の場に近いコンビニなどにおいてもこれによる決済が実践されている。

一方で、公共セクターが、例えばマイナンバーカードに個人の顔写真を登録させようとしたときや、押印やサインの代わりに指紋押捺をさせようとすると市民社会はマスメディアを巻き込んだ抵抗運動とも言えるムーブメントを起こしたが、Appleへのそれらの提供に対しては全くと言っていいほど口を詰むんだままである。その仮説の一つの理由として「便利さとのトレードオフ」を設定したが、エモスタの事例によって監視者と被監視者が「世界観の合意を強制できる」状況が生じると、つまり、被監視者が許容し得る等価交換ができると全く素直に個人を特定する情報を提供することがわかった。これは同様にテロなどの危機に対する監視カメラの地域社会への導入とその監視についても同じことが言える。よって民間レベルの消費行動においては、前述した様に「高品質」なデジタルマーケティングによるリマーケティングが誕生し宣伝すら感謝され得るコンテンツになる環境が増醸されたのである。ゆえに、人々がFaceIDを毎日何回も作動させるべく、便利と引き換えに、承諾、承認をした上でプライバシーに直接絡む個人情報を「喜んで」提供するのである。

しかし、中国人アクティビストの拘束の事例にある様に、民間企業とはいえ、上場企業である以上、ステークホルダーの内、株主に過度に資する意思決定は止むを得ず、公権力の行使に対して迎合してしまう例などを見るに、安易にビックデータの管理および分析を公共セクター、または民間

セクターに委ねることへの警戒は必須であるともいえる。

また、そもそも顔のデータや個人情報を保存、分析されることになぜ反対するのだろうか。無論憲法上で認められた基本的人権ではあるものの、今一度、根本的にそのことを考えなければならない。犯罪者がそれを嫌うのは理解できるが、善良な市民が個人情報を分析されたからと言って「気持ち悪さ」以外に一体何が起こるのかという究極的で危険とも思われる問題の再考に対して、これからの市民社会での思考停止は禁物である。何故ならばキーボード入力よりも右手の親指だけのフリック入力の方がスピードが速くストレスのないデジタルネイティブ世代においては圧倒的にこれらの感覚が異なると想定されるからである。憲法上保証されている基本的人権はしっかりと担保した上で、しかし、新しい世代が新しい技術とプライバシーの関係、または、「便利さとのトレードオフ」の新しい常識を更新していくことは容易に想像できるのだ。

そこで少なくても私たちが挑まなくてはならない仕事は、この手の議論を法学や社会学などの社会科学上だけの議論に留めずに、必ず工学を含む学際領域で取り組むべきことであり、さらに、全力で反論をする際には必ずや次のデジタルネイティブ世代を想定した代替えのソリューションを提案する、この2点を心がけるべきである。

注

1）http://www.sej.co.jp/company/news_release/news/2018/20181113_copy_2_copy_copy.html
2）平成7年12月15日／最高裁判所第三小法廷／判決／平成2年（あ）848号「外国人指紋押捺拒否事件上告審判決」など
3）https://www.counterpointresearch.com/iphone-x-drove-apples-revenue-super-cycle/
4）2006年2月17日「朝日新聞」（朝刊）2面（東京本社版）他
5）2013年4月2日「中央日報／中央日報日本語版」コラムなど
6）https://diamond.jp/articles/-/174282
7）https://www.epo.org/news-issues/news/2012/20120229.html
8）The IPKat: http://ipkitten.blogspot.com/2012/02/patent-translate-epo-and-google-launch.html
9）https://www.panasonic.com/global/olympic/ja/london/support/security.html
10）https://sol.panasonic.biz/solution/security/facepro.html
11）https://www.jeita.or.jp/japanese/stat/drive/
12）https://emosta.com/team/

主な参考文献

田島泰彦・斎藤貴男／編『超監視社会と自由』（花伝社）2006
ブルース・シュナイアー／著『超監視社会』（草思社）2016
ケビン・ミトニック，ロバート・バシモ／著『超監視社会で身をまもる方法』（日経BP）2018
武邑光裕／著『さよなら，インターネット』（ダイヤモンド社）2018
高柳寛樹／著『まったく新しい働き方の実践～「IT前提経営」による「地方創生」～』（ハーベスト社）2017
高柳寛樹／著『メディア産業における根幹技術の決定・採用過程と，それに働く「文化装置」に関する一考：テレビとインターネットの事例を中心に』応用社会学研究No.55（立教大学社会学部）2010
高柳寛樹／著『メディアの技術決定過程の研究における，「標準化」の類型：「オープン標準」という提案』応用社会学研究No.56（立教大学社会学部）2014
高柳寛樹／著『メディア技術のイノベーションと社会受容のパターンについての一考：地デジ化がもたらした人文的ディスクールの思考から』応用社会学研究No.58（立教大学社会学部）2016
高柳寛樹／著『日本の情報産業を支えるソフトウェア産業におけるベンチャー企業のリスクと成長性の類型化の研究』応用社会学研究No.51（立教大学社会学部）2009
高橋利枝，本田量久，寺島拓幸／著『デジタル・ネイ

ティヴとオーディエンス・エンゲージメントに関する一考察：デジタル・メディアに関する大学生調査より』応用社会学研究No.50（立教大学社会学部）2008
イーライ・パリサー／著『フィルターバブル―グーグル・パーソナライズ・民主主義―』（早川書房）2016
ジョン・キム／著『ウィキリークスからフェイスブック革命まで逆パノプティコン社会の到来』（ディスカヴァー携書）2011
ジェフリー・ムーア／著『キャズム』（翔泳社）2002
前田陽二／著『未来型国家エストニアの挑戦―電子政府がひらく世界』（NextPublishing）2016
古瀬幸広，広瀬克哉／著『インターネットが変える世界』（岩波書店）1996
水越伸／著『新版デジタル・メディア社会』（岩波書店）2002

著者略歴

高柳寛樹（たかやなぎ・ひろき）
1976年東京生まれ、長野県白馬村在住。株式会社ウェブインパクト／取締役ファウンダー、株式会社ウェブインパクトR&D／代表取締役、アロワナパートナーズ株式会社／代表取締役、ガーディアン・アドバイザーズ株式会社／パートナー、立教大学大学院／特任准教授（2019-）、立教池袋高等学校／兼任講師、一般社団法人ネットリテラシー検定機構／理事、SNOWTECH／共同創業者などを兼務。「IT前提経営®（Tech Driven Management）」の提唱者。専門は情報社会論、情報産業論、技術経営論など。情報社会学者として研究教鞭活動をしながら実践の場として20年以上に渡り複数のテクノロジー企業の経営をする。情報通信学会、公共政策学会、日本ベンチャー学会、マス・コミュニケーション学会、日本マネジメント学会などに参加。日本アーティスト協会／正会員。https://hiroki.st/profile/